(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 184 773 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.03.2002 Bulletin 2002/10

(51) Int Cl.[7]: **G06F 1/00, G08B 13/12**

(21) Application number: **01307299.6**

(22) Date of filing: **28.08.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **01.09.2000 US 654543**

(71) Applicant: **International Business Machines Corporation**
Armonk, N.Y. 10504 (US)

(72) Inventors:
- **Butturini, Giuseppe,**
  c/o IBM United Kingdom Ltd.
  Winchester, Hampshire SO21 2JN (GB)
- **Farquhar, Donald S.,**
  c/o IBM United Kingdom Ltd.
  Winchester, Hampshire SO21 2JN (GB)
- **Fontana, Fulvio, c/o IBM United Kingdom Ltd.**
  Winchester, Hampshire SO21 2JN (GB)

(74) Representative: **Moss, Robert Douglas**
IBM United Kingdom Limited Intellectual Property Department Hursley Park
Winchester Hampshire SO21 2JN (GB)

(54) A method of securing an electronic assembly against tampering

(57) A method for forming a security enclosure comprises folding a flexible tamper respondent cloth around an electronic assembly. An adhesive on the inner folded surfaces of the cloth temporarily retains the folds. The enclosure is then exposed to heat and pressure to promote improved adhesion strength of the adhesive, thereby improving fold retention.

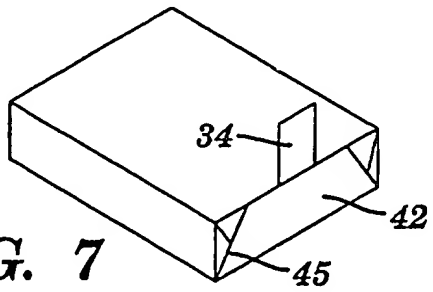

FIG. 7

EP 1 184 773 A1

Description

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention relates generally to the detection of intrusions into electronic assemblies, and more particularly, to the retention of a security enclosure capable of detecting such intrusions.

BACKGROUND OF THE INVENTION

[0002] In electronic network commerce applications, it is a requirement to protect the contents of the associated computer systems from being unlawfully read or modified. It is conventional practice to provide certain encryption schemes in which data is transmitted and received in an encrypted form and only authorized people who have the encryption key codes may read or modify the data. However, an unauthorized person with sufficient skills and knowledge may attempt to bypass software encryption controls by making a physical attack against the computer hardware to attempt a direct interrogation of the memory components and other devices. Defense from these types of attacks requires that tamper resistant physical packaging be provided for critical encryption components, in such a way that unauthorized attempts to gain entry are detected and encryption key codes are immediately erased. One means of providing physical protection against intrusion is the use of an electrical grid surrounding the encryption module, which when broken triggers the requisite signal to disable the unit. It is known in the art to surround and protect an encryption module with a membrane consisting of one or more flexible dielectric layers having electrically conductive traces thereon. The membrane is electrically connected to the module, then wrapped, folded and bonded around the module, wherein a sticky pressure sensitive bonding adhesive adheres the membrane around the module. The traces are intentionally made fragile so that they are damaged if an attempt is made to remove the membrane. Further the membrane may be potted in a molding material, which offers further protection as its removal would also damaged the traces.

[0003] While the membrane must meet the physical security requirements, it must not be so sensitive that it falsely triggers the erasure of the key codes as a result of handling during the manufacturing assembly process, or subsequently due to environmental conditions associated with changes in temperature, humidity or atmospheric pressure. Accordingly, one of the drawbacks in the current art is that the security membranes intended for wrapping, folding, and bonding to an enclosure may be too stiff to readily fold as a result of the thickness and other properties of the various layers. As a result, during the assembly folding process, a fold may be completed but the stiffness of the membrane may result in poor retention of the fold, as the elastic strain energy associated with bending the membrane overwhelms the adhesive strength of the bonding adhesive. This can result in two conditions. First, the unfolding can damage the fragile circuit traces as the adhesive pulls against them during unfolding of the membrane. Second, unfolding can produce the formation of openings or tunnels through which the subsequently applied molding materials may leak into the interior of the enclosure, resulting in the possibility of an immediate failure or potentially a reduction in reliability of the internal components.

[0004] Thus, there is a need for better means for performing the assembly wrapping, folding, and bonding operation in such a way that the membrane is not damaged, and that molding material can not subsequently leak into the interior of the enclosure. Contrary to meeting this requirement stands the fact that the available membrane materials have certain physical properties associated with their materials selection and cross-sections that can not be readily altered, and further the fact the conductive traces are intentionally fragile so as to detect any security attack.

DISCLOSURE OF THE INVENTION

[0005] Accordingly, the present invention provides a method of securing an electronic assembly against tampering, comprising: wrapping the assembly in a tamper respondent sheet to form an enclosure for the assembly; providing overlapping portions of the sheet with a heat curable adhesive; clamping the enclosed assembly to maintain the overlapped portions of the sheet in contact with the adhesive; and heating the enclosed assembly to heat cure the adhesive thereby to ensure integrity of the enclosure.

[0006] A first embodiment provides a method of forming a security enclosure, comprising: providing an electronic assembly; enclosing the assembly in a tamper respondent wrap, such that the wrap forms fold lines at a first and second end of the assembly; placing the enclosed assembly in a fixture, wherein the fixture comprises a base upon which the assembly rests, a first stationary arm mounted on the base holding the fold lines at the first end of the assembly, a second arm slidably mounted on the base, and a traversing mechanism to bias the second arm toward the fold lines at the second end of the assembly; and heating the enclosed assembly.

[0007] A second embodiment provides a method of producing a tamper respondent enclosure, comprising: enclosing a cryptographic processor in a tamper respondent sheet, wherein an adhesive material secures the enclosure; holding the enclosed cryptographic processor such that the adhesive material remains intact; and applying heat to the enclosed cryptographic processor to strengthen the adhesive material.

[0008] A third embodiment provides a method of forming a security enclosure, comprising: providing a circuit card; enclosing the card in a tamper respondent cloth, wherein an adhesive secures fold lines of the cloth; hold-

ing the fold lines of the cloth to maintain adhesive contact; and heating the enclosed card.

[0009] A fourth embodiment provides a method of assembling a security enclosure comprising: providing a fixture; providing an enclosure having a cloth member thereon; placing the enclosure in the fixture; heating the enclosure; and removing the enclosure from the fixture.

[0010] A fifth embodiment provides an apparatus for securing a security enclosure, comprising; a base upon which a security enclosure rests; a first stationary arm mounted on the base, which holds a first end of the security enclosure; a second arm slidably mounted on the base; and a traversing mechanism to bias the second arm toward a second end of the security enclosure.

[0011] The foregoing and other features and advantages of the invention will be apparent from the following more particular description of the embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The embodiments of this invention will be described in detail, with reference to the following figures, wherein like designations denote like elements, and wherein:

Fig. 1 depicts a top view of a tamper respondent wrap in accordance with the present invention;

Fig. 2A depicts an electronic assembly in accordance with the present invention;

Fig. 2B depicts the electronic assembly of Fig. 2A having an enclosure therearound in accordance with the present invention;

Fig. 3 depicts a first step in enclosing the assembly of Fig. 2A within the wrap of Fig. 1 in accordance with the present invention;

Fig. 4 depicts a second step in enclosing the assembly of Fig. 2A within the wrap of Fig. 1 in accordance with the present invention;

Fig. 5 depicts a third step in enclosing the assembly of Fig. 2A within the wrap of Fig. 1 in accordance with the present invention;

Fig. 6 depicts a fourth step in enclosing the assembly of Fig. 2A within the wrap of Fig. 1 in accordance with the present invention;

Fig. 7 depicts a fifth step in enclosing the assembly of Fig. 2A within the wrap of Fig. 1 in accordance with the present invention;

Fig. 8 depicts a graph illustrating the bending modulus of the wrap of Fig. 1 in accordance with the present invention; and

Fig. 9 depicts a clamping device used in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0013] Referring to the drawings, Fig. 1 shows a tamper respondent wrap or cloth 10 as known and used in the art. The tamper respondent cloth 10 may be a sheet of composite material similar to one made by a division of W.L. Gore (Dundee, Scotland), as described in a patent to MacPherson (US 5,858,500). In particular, the tamper respondent cloth 10 comprises a laminate formed of a number of separate layers, including a delamination respondent layer, and a pierce and laser respondent layer.

[0014] The respondent layers of the tamper respondent cloth 10 comprise electrically responsive line elements that are disposed on a film material. The pierce and laser respondent layer is intended to detect efforts to penetrate the security enclosure by means of forming a small hole through the tamper respondent cloth 10. The delamination respondent layer is intended to detect efforts to peel the tamper respondent cloth 10 away from the outer surface of the inner enclosure. The delamination respondent layer is provided with an adhesive characteristic such that peeling it away from a surface will damage the electrically responsive materials therein. These respondent layers are adhered together by means of an adhesive. Thus the tamper respondent cloth 10 comprises respondent film layers that are bonded together with an adhesive. Moreover, an adhesive is provided to retain the folded and overlapping portions upon folding. A top view of one such respondent layer is shown in Fig. 1. The layer includes an electrically insulating film 12, made of polyester film or other similar material, having a plurality of diagonally extending ink traces or lines 14 formed on a first and second side of the film 12 (one side shown). The lines 14 are formed by printing carbon loaded polyester ink on the surface of the film 12. The lines 14 printed on each side of the film 12 are then selectively connected at the edges 13 of the film 12. The lines 14 form a plurality of continuous conductors which break easily if attempts are made to penetrate the delamination respondent layer or the pierce and laser respondent layer.

[0015] Connection between the lines 14 and an enclosure monitor of the electronic assembly (described *infra*) is provided by an integrated ribbon cable 18. Like the lines 14, the ribbon cable 18 is formed by printing carbon loaded polyester ink onto a first surface of the layer 12. Connectors 16, also formed on the first surface of the layer 12, make the connection between the ribbon cable 18 and the lines 14.

[0016] Fig. 2A shows an electronic assembly such as a cryptographic processor card 20 in accordance with the present invention. The cryptographic processor card

20 contains an encryption module 22 which carries the secured sensitive information, a memory 24 which stores a key or code necessary to access the stored information in the encryption module 22, an erase circuit 26 which erases the stored information in the encryption module 22 in the event the tamper respondent cloth 10 around the cryptographic processor card 20 is breached, an enclosure monitor 28 which monitors the resistance of the lines 14 of the cloth 10 and activates the erase circuit 26 in the event a breach is detected, and a battery 30, all of which are mounted on a printed circuit board 32. The cryptographic processor card 20 further includes a plurality of connecting or ribbon cables 34 (one of which is shown), which are used to connect multiple enclosures to one another on a board (not shown), as known in the art.

[0017] The cryptographic processor card 20 may then be positioned inside a housing 100 comprising for example a top half 102 and a bottom half 104 of a sheet metal box, as illustrated in Fig. 2B. The two halves 102, 104 may be joined together, and include openings 106 as need to insert electrical cables into the processor card 20. The housing 100 may be designed to provide a suitable surface for wrapping the tamper respondent cloth 10. The tamper respondent cloth 10 is then wrapped around the housing 100 containing the cryptographic processor card 20 in a manner similar to that of a gift-wrapped present, as illustrated in Fig. 3. The cloth 10 overlaps near the middle of the cryptographic processor card 20, on the underside of the card 20. The connectors 16 and ribbon cable 18 (Fig. 1) are wrapped within the cloth 10 such that the ribbon cable 18 interconnects with the enclosure monitor 28 within the enclosure.

[0018] A top flap 36 at each end of the cloth 10 is folded down over the ends 38 of the housing 100 containing the card 20 (one end 38 is shown in Fig. 4 for ease of illustration). An adhesive on the inner surface of each top flap 36 adheres each top flap 36 to the respective ends 38 for ease of assembly. As illustrated in Fig. 5, the connection cable 34 at the one end is folded upward to abut the folded top flap 36 (noting that only one end of the cryptographic processor card 20, the end nearest the encryption module 22, has the connection cable 34 extending therefrom in the current illustration, however, the present invention is not intended to be limited to the quantity nor location of the connection cable shown).

[0019] As illustrated in Fig. 6, the side flaps 40 at each end 38 of the housing 100 containing the card 20 are folded inward to overlap the top flap 36 at each end 38, and the connection cable 34 at the one end. As with the top flap 36, each side flap 40 includes an adhesive on the inner surface of each flap 40 such that each side flap 40 adheres to each top flap 36 at each end 38 of the housing 100 containing the card 20, and the connection cable 34 at one end 38 of the card 20, during assembly. Each bottom flap 42 is then folded upward to overlap the top 36 and side flaps 40, as well as the connection cable 34 (at the one end 38 of the card 20), as illustrated in Fig. 7. As with the top and side flaps 36, 40, each bottom flap 42 includes an adhesive on the inner surface of the flap 42 to adhere each bottom flap 42 to the connection cable 34 and/or the side and top flaps 36, 40, thereby forming a complete enclosure for the card 20.

[0020] It should be noted that the present invention is not intended to be limited to the order of folding the tamper respondent cloth 10 around the card 20 described above. In contrast, the side flaps 40 may be folded inward first, followed by either the top 36 or bottom flaps 42. Alternatively, the bottom flap 42 may be folded upward first, followed by either the side flaps 40 or the top flap 36, and so on.

[0021] The enclosure of Figure 7, having fold lines 45 at each end 38 thereof, is then placed in a clamping device or fixture 46 similar to the one shown in Fig. 9. The clamping device 46 includes a base 48 and a plurality of legs 50 thereunder. A stationary clamping arm 52 is securely mounted to a first end of the base 48. A traversing clamping arm 54 is slidably mounted to the base 48. A biasing or traversing mechanism 56, located at a second end of the base 48, is connected to the traversing clamping arm 54. The traversing mechanism 56, comprising a biasing screw, a hydraulic mechanism, an electro-mechanical sensor motor, etc., functions to bias the traversing clamping arm 54 toward and/or away from the stationary clamping arm 52.

[0022] In practice, the enclosure of Figure 7 is placed on the base 48 of the clamping device 46, such that one end of the enclosure is positioned against the stationary clamping arm 52. The traversing clamping arm 54 is then biased toward the other end of the enclosure via the biasing mechanism 56.

[0023] Once the traversing clamping arm 54 of the clamping device 46 is adjusted such that the enclosure fits snugly between the traversing clamping arm 54 and the stationary clamping arm 52, the enclosure and clamping device 46 are exposed to a temperature of approximately 40-90 °C, and preferably between 50-70 °C (because the ink lines 14 may begin to soften and reflow at temperatures above approximately 80 °C), 60 °C being the optimal temperature, for approximately 1 hour (refer to the temperature chart of Fig. 8). The enclosure is then removed from the clamping device 46. Thereafter, the enclosure may undergo additional processing as known in the art, i.e., applying a polyurethane coating, etc.

[0024] Heating the tamper respondent cloth 10 initially causes the layers of adhesive to soften, thereby allowing the pierce and laser respondent layer to slide past the delamination respondent layer in the fold areas such that the cloth 10 bends more easily. Upon continued heating the adhesive cross-links or cures due to thermal ageing, thereby making the adhesive become more solidified. After removing the heat, the adhesive continues to harden in the folded position during cooling. As a result, the folded cloth 10 forming the enclosure

exhibits improved fold retention and reduced stress. And unlike the previous methods of forming enclosures, the cloth 10 does not come un-wrapped during processing. Accordingly, the subsequent encapsulant material, e.g., a polyurethane coating, will not flow past the folds into the inner enclosure to damage the cryptographic processor card 20, as often happens with conventional methods.

[0025] It should be noted that the enclosure of Figure 7 described and illustrated herein is only one example of the type of enclosure that may be use in combination with the present invention. The present invention is in no way intended to be limited to use in conjunction with electronic assemblies of this size, shape and form. Rather, the enclosure may take the form of a wedge-shaped enclosure, a cuboid, a cube, etc.

Claims

1. A method of securing an electronic assembly against tampering, comprising:

   wrapping the assembly in a tamper respondent sheet to form an enclosure for the assembly;

   providing overlapping portions of the sheet with a heat curable adhesive;

   clamping the enclosed assembly to maintain the overlapped portions of the sheet in contact with the adhesive; and

   heating the enclosed assembly to heat cure the adhesive thereby to ensure integrity of the enclosure.

2. A method as claimed in claim 1 in which the enclosed assembly is heated at between 40°C and 90°C.

3. A method as claimed in claim 2 in which the enclosed assembly is heated at 60°C.

4. A method as claimed in any preceding claim in which the enclosed assembly is heated for one hour.

5. A method as claimed in any preceding claim wherein the tamper respondent sheet comprises two layers joined by an adhesive, said heating step initially causing softening of the adhesive joining the two layers to permit relative movement thereof.

6. A method as claimed in any preceding claim wherein said wrapping step produces fold lines in the tamper respondent sheet material and the bending modulus of the sheet material decreases with temperature so that said heating step reduces any tendency of the sheet to unfold.

7. A method as claimed in any preceding claim wherein the tamper resistant sheet comprises a flexible material coated with a conductive pattern, the sheet being formed with a ribbon cable portion, the method comprising the step of electrically connecting the ribbon cable portion to an enclosure monitor within the electronic assembly for detecting breach or delamination of the sheet.

8. A method as claimed in claim 7 including the step of forming the conductive pattern on the sheet by printing carbon loaded polyester ink on to a surface of the sheet.

9. A method as claimed in any preceding claim in which the overlapping portions of the sheet are temporarily retained together by the adhesive prior to said clamping and heating steps.

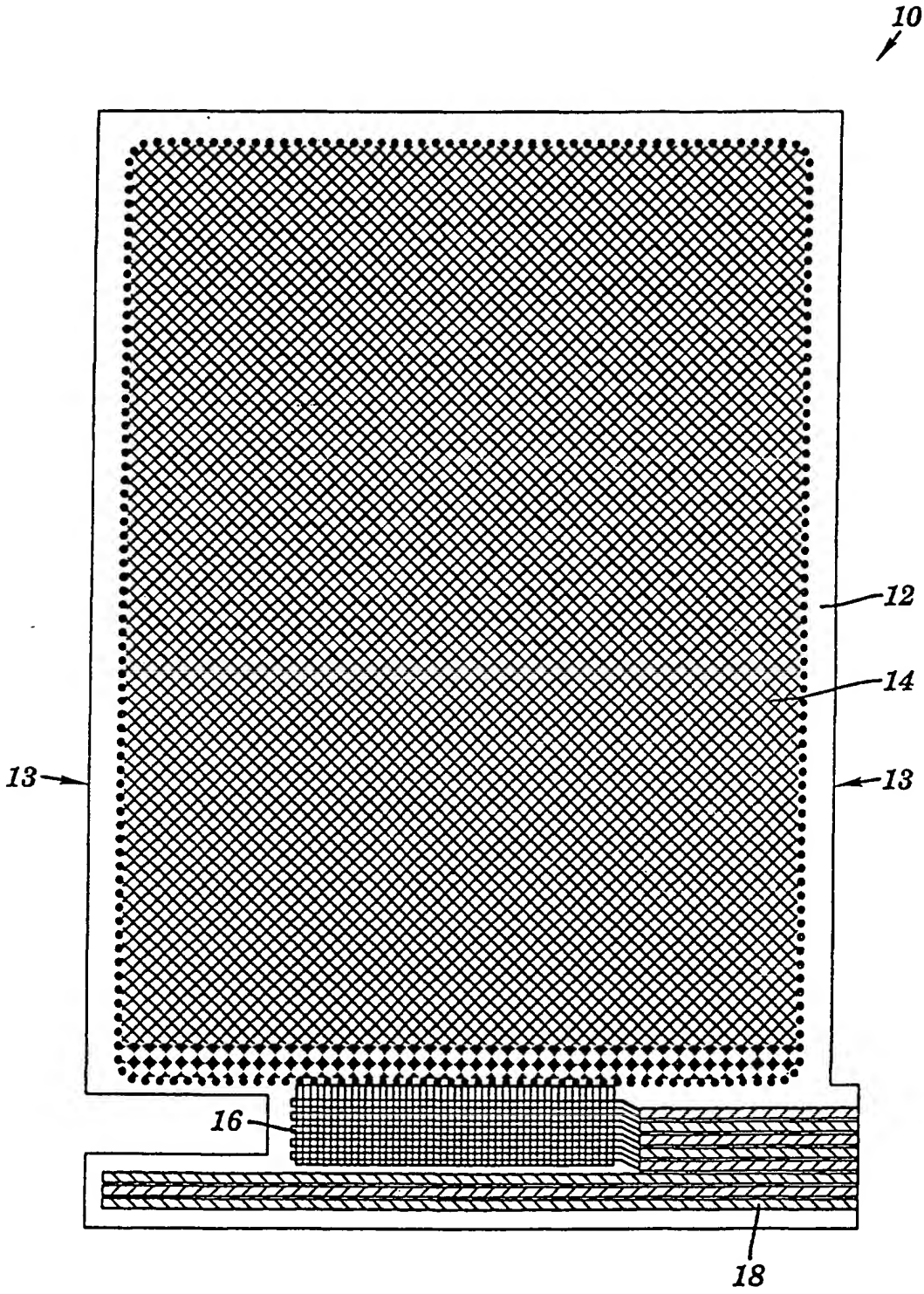

FIG. 1

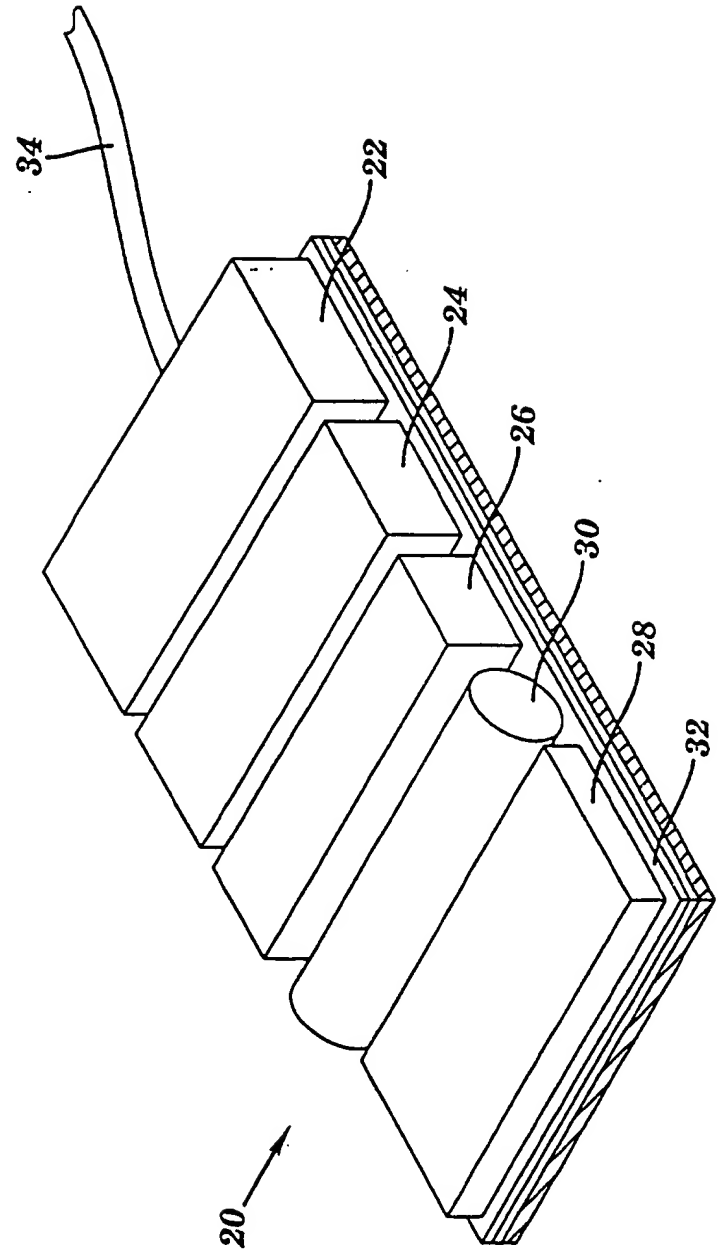

FIG. 2A

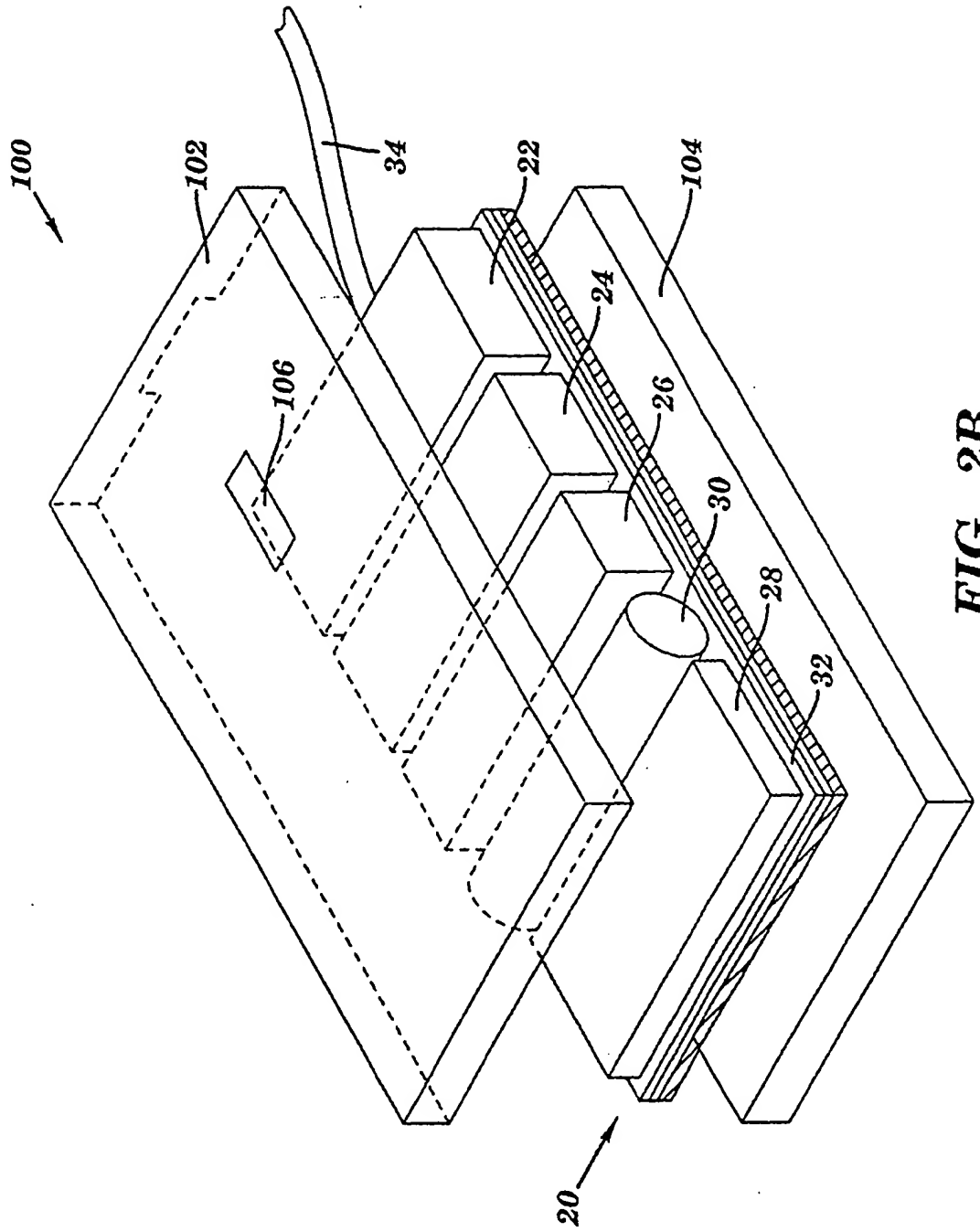

FIG. 2B

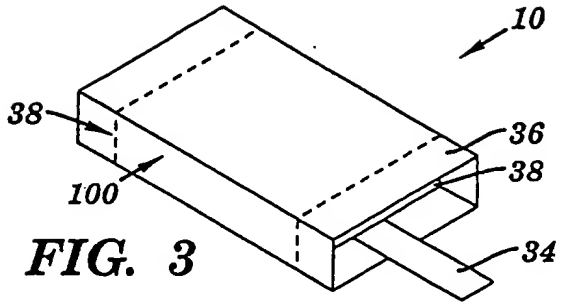

FIG. 3

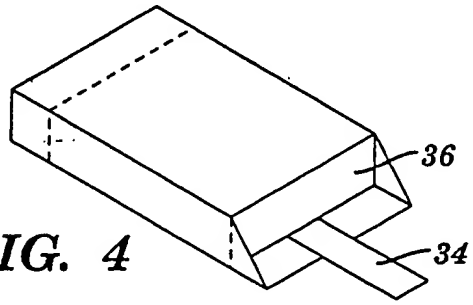

FIG. 4

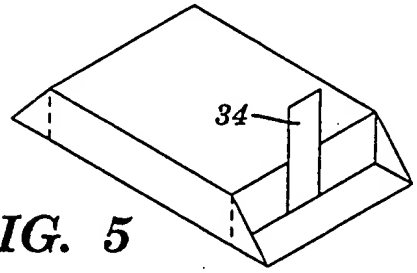

FIG. 5

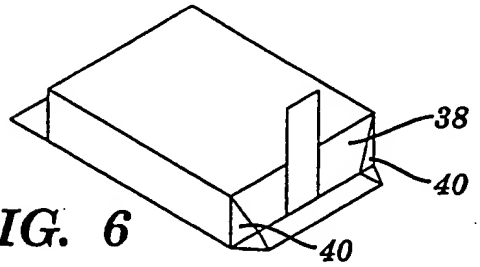

FIG. 6

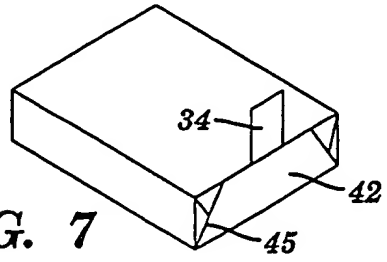

FIG. 7

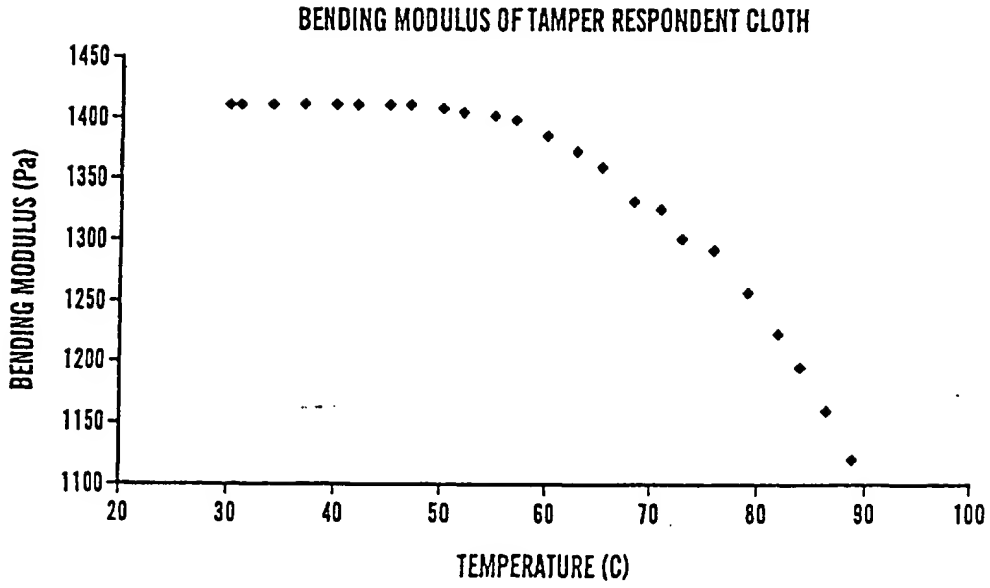
BENDING MODULUS OF TAMPER RESPONDENT CLOTH
BENDING MODULUS (Pa)
1450
1400
1350
1300
1250
1200
1150
1100
20
30
40
50
60
70
80
90
100
TEMPERATURE (C)

FIG. 8

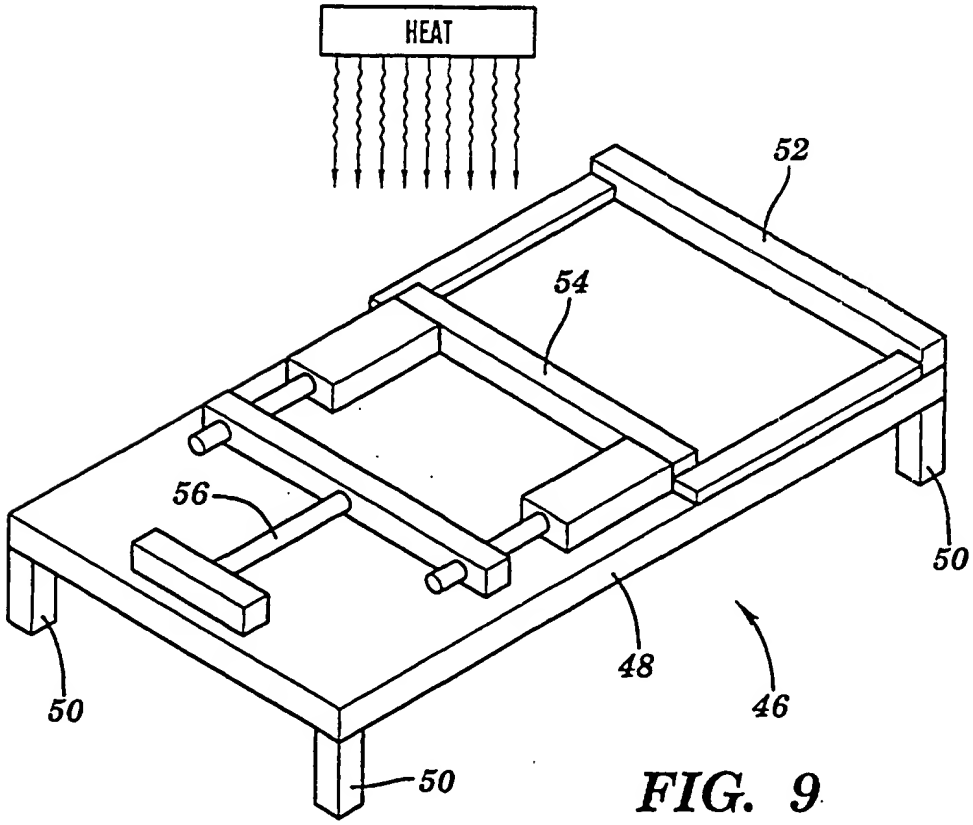
HEAT
52
54
56
50
48
46
50
50

FIG. 9

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 30 7299

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
P,X	EP 1 045 352 A (W L GORE & ASSOCIARES S R L) 18 October 2000 (2000-10-18) * column 3, line 31 - line 44 * * column 5, line 42 - column 7, line 17 * * column 8, line 17 - line 54; figures 1,2,4 *	1,2,6-9	G06F1/00 G08B13/12
A	GB 2 270 785 A (GORE & ASS) 23 March 1994 (1994-03-23) * page 14, paragraph 2 - page 17, paragraph 1; figures 2,4,5 *	1-9	
D,A	GB 2 275 914 A (GORE & ASS) 14 September 1994 (1994-09-14) * abstract *	1	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G06F
G08B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	5 December 2001	Moens, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 30 7299

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-12-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1045352 A	18-10-2000	EP 1045352 A1	18-10-2000
GB 2270785 A	23-03-1994	AU 670324 B2	11-07-1996
		AU 4976893 A	12-04-1994
		CA 2145085 A1	31-03-1994
		DE 69305653 D1	28-11-1996
		DE 69305653 T2	13-03-1997
		EP 0663096 A1	19-07-1995
		WO 9407221 A1	31-03-1994
		JP 8504043 T	30-04-1996
		US 5539379 A	23-07-1996
GB 2275914 A	14-09-1994	AU 688707 B2	12-03-1998
		AU 1491697 A	15-05-1997
		AU 676540 B2	13-03-1997
		AU 6149794 A	26-09-1994
		CA 2157800 A1	15-09-1994
		DE 69410253 D1	18-06-1998
		DE 69410253 T2	07-01-1999
		EP 0689703 A1	03-01-1996
		WO 9420935 A1	15-09-1994
		GB 2297540 A ,B	07-08-1996
		JP 8508121 T	27-08-1996
		US 5858500 A	12-01-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82